AMENDMENTS TO THE SPECIFICATION

Amend the paragraph found on page 4, lines 16-20 as follows:

A scenario wherein the authenticity message is communicatable to the terminal ~~but eh~~ by the server, the authenticity output message preferably having been transmitted to the server by the user, refers to a situation when the personal device is not even writable by the user. This opens the invention to the field of prefabricated, non-amendable personal device, such as preprogrammed or prewritten smartcards or magnetic cards.

a1

Amend the paragraph found from page 5, line 8 through page 6, line 17 as follows:

The invention is related to a system which allows a user to authenticate unknown terminals. The user can hereby detect if a terminal he wants to use is a fake terminal or if it is a legal terminal and can be trusted. Only trusted terminals should be used to perform security-sensitive actions via the terminal. The invention uses a first authentication step wherein the terminal authenticates itself to a server. The authentication is either initiated simply by coupling a personal device to the terminal, or by some additional action performed by the user. The user can, for example, additionally press one or more buttons or keys on the terminal or on the personal device, wherever such input means are present. For authentication, any known ~~any know~~ authentication system can be used (e.g., using a private-public key system). Depending on whether the personal device has its own output means, such as a loudspeaker or a screen, the final message, whether the terminal can be trusted or not, can be output on the personal device or on the terminal itself. Since the user

trusts his personal device, this message preferably should come from the device itself. In the case where the device has no output means of its own, this message can originate in the device and be transmitted from there to the terminal. The user can input authentication information into his personal device, which can then be fully or partially transmitted to the terminal. In the end, the terminal may use the transmitted information to give out the authenticity output message. After the first authentication step follows a second authentication step, wherein the server authenticates itself to the personal device, if there is one. Upon success of both authentication steps, the authenticity output message can be given to the user. If the personal device has no writing capability, the authentication information, also called the authentication vector, can be transferred by the user via a trusted channel to the server. Upon successful authentication, the server can then output some message to the terminal to make it output the authenticity output message. The message from the server to the terminal can therefore be the authenticity output message itself, part of it, or any other kind of message that effects issuance of the authenticity output message to the

user. In the case where the user has no own personal device, the method can be used to transmit to the server the authentication vector before approaching the terminal. The user has agreed with the server on one or more tuples of challenge-response authentication vector type. The authentication is performed via the challenge-response principle and upon successful authentication, the server finally issues or has issued the authenticity output message via the terminal. The second messaging step, i.e., the output of the authenticity output message, is preceded by a first messaging step which comprises the issuance of a message from the server. The message of the first messaging step indicates that the terminal can be trusted.

Amend the paragraph found from page 7, line 9 through page 8, line 6 as follows:

In the following, general scheme of the present invention and various exemplary embodiments thereof are described. A typical system in which the present invention can be used is illustrated in Figure 1. The user 1 accesses a server system 5 from a public untrusted terminal 6. This terminal has a terminal output device 3, such as a screen or the like, via which ~~is~~ it communicates with the user. This terminal output device also has means for the user to communicate with the terminal 6, e.g., a keyboard. The terminal 6, respectively terminal output device 3, is connected to the server 5 via a network 14 ~~network 4~~, which in its simplest form can be a direct line. For this purpose of accessing the server, the user 1 has an account on a central server system 5 which he trusts to correctly authenticate a public terminal 6. Public terminals are tamper-resistant but an attacker can easily replace a legal terminal 6 with a fake terminal or install a new fake terminal in a plausible location. The server 5 knows about legal

terminals 6 and can authenticate them. Information necessary for a user 1 to authenticate the central server 5 (and, where necessary, information needed for the central server 5 to authenticate a user 1) is set up during known user registration or other initialization steps (e.g., agreeing on a shared key). Once an entity authenticates another, a confidential, authenticated channel is established as a result. In other words, an attacker cannot hijack a authenticated channel resulting from the authentication procedure. The symbols U, T, and S, are herein used to identify a user 1, a terminal 6, and a central server 5, respectively. When the user 1 has a trusted personal device 2, it is denoted by D. This notation is illustrated in Figure 1.

Amend the paragraph found from page 11, line 17 through page 12, line 16 as follows:

~~The scheme described in the present Section 2.1 can be summarized as follows. Details are~~ As schematically illustrated in Figure 3, the ~~3. The~~ personal device 2 is equipped with means such that it can be coupled to a terminal 6. It furthermore comprises code which, when being executed in the device 2, performs a method for establishing a trustworthy connection between a user 1 and the terminal 6. This terminal 6 is connected to and authenticatable by at least one server 5 which is authenticatable by the device 2. If the device 2 is coupled to the terminal 6, which coupling may be performed by physical, optical, wire-bound, or wireless means, the following steps are carried out:

- A first authentication step AI is initiated during which said terminal 6 authenticates itself to the server 5. Upon success of this initiation, a first authenticated trusted connection c1 is established between said server 5 and said terminal 6.

- Then, a second authentication step AII is initiated during which - via said established first authenticated trusted connection c1 - the server 5 authenticates itself to the device 2. Upon success of this authentication, a second authenticated trusted connection c2 is established between the server 5 and the device 2.

- Then, a terminal authenticity message (m_t) is received by the device 2 during a first messaging step MI. This message is received from the server 5 via the established second authenticated trusted connection c2 and confirms the established authenticity of the terminal 6.

a4

- Then, during a second messaging step MII, an authenticity output message (m_o) is provide by the device 2 to the user 1. This is done via an output of the device 2 and/or via a terminal output 3 of the terminal 6.

/

Amend the paragraph found from page 12, line 17 through page 13, line 5 as set forth below:

The personal device 2 might comprise ~~comprises~~ stored predetermined authentication information (vec) which can be sent to the terminal 6 for it to create the authenticity output message (m_o). Usually, the authenticity output message (m_o) is sent by the server 5 to the terminal 6. This authenticity output message (m_o) might comprise visible, audible, or tactile information (e.g., one or more of the following: background color, foreground color, background pattern, sound, letters, numbers). Likewise, the authenticity output message (m_o) might comprise at least one value for lookup in a table 4 which is stored in the terminal 6, for example. The authenticity output message (m_o) might have been transmitted by the user 1 to the server 5. This is preferably done via a trusted communication connection cs. The authentication steps AI, AII, and AIII might be bidirectional.

Q5

Amend the paragraph found on page 13, lines 13-20 as follows:

The server 5 is connected to the terminal 6 via a network or link and is able to authenticate the terminal 6 during the first authentication step AI. After the first authentication step AI a first authenticated trusted connection c1 is established between the server 5 and the terminal 6. The server 5 ~~is~~ furthermore has to be enabled to authenticate itself to the device 2 during the second authentication step AII such that the second authenticated trusted connection c2 is established. Then, the server 5 sends the terminal authenticity message (m_t) to the device 2 via the established second authenticated trusted connection c2, to confirm the established authenticity of the terminal 6.

Amend the paragraph found on page 14, lines 1-8 as follows:

Now a scenario is considered where a user 1 is equipped with a device 2, such as an integrated circuit card (e.g. a smartcard), which has no output capability. One could try to use the same solution for this scenario as well. However, the problem arises in step 6 since D does not have its own display. Consequently, it does not have a trusted path to U. There may be devices with other types of trusted paths (e.g., mobile phones could use a speech synthesizer to communicate the message to U), in which case the previous solution ~~described in section 2.1~~ could still be used. Standard smartcards, however, have no such output mechanism. Hence one needs to modify the solution described above.